WATERMARK SYSTEMS AND METHODS

Related Application Data

This application claims priority to provisional application 60/257,822, filed December 21, 2000.

Field of the Invention

The present disclosure memorializes various improvements relating to digital watermarking technology and applications.

Background of the Invention

The present disclosure memorializes various improvements relating to digital watermarking.

Digital watermarking is the science of encoding physical and electronic objects with plural-bit digital data, in such a manner that the data is essentially hidden from human perception, yet can be recovered by computer analysis. In physical objects, the data may be encoded in the form of surface texturing, or printing. Such marking can be detected from optical scan data, e.g., from a scanner or web cam. In electronic objects (e.g., digital audio or imagery – including video), the data may be encoded as slight variations in sample values. Or, if the object is represented in a so-called orthogonal domain (also termed "non-perceptual," e.g., MPEG, DCT, wavelet, etc.), the data may be encoded as slight variations in quantization values or levels. The present assignee's patent 6,122,403, and application 09/503,881, are illustrative of certain watermarking technologies.

Watermarking can be used to tag objects with a persistent digital identifier, and as such finds myriad uses. Some are in the realm of device control – e.g., tagging video data with a do-not-copy flag that is respected by compliant video recorders. (The music industry's Secure Digital Music Initiative (SDMI), and the motion picture industry's Copy Protection Technical Working Group (CPTWG), are working to establish standards relating to watermark usage for device control.) Other watermark applications are in the

field of copyright communication, e.g., indicating that an audio track is the property of a particular copyright holder.

Other watermark applications encode data that serves to associate an object with a store of related data. For example, an image watermark may contain an index value that serves to identify a database record specifying (a) the owner's name; (b) contact information; (c) license terms and conditions, (d) copyright date, (e) whether adult content is depicted, etc., etc. (The present assignee's MarcCentre service provides such functionality.) Related are so-called "connected content" applications, in which a watermark in one content object (e.g., a printed magazine article) serves to link to a related content object (e.g., a web page devoted to the same topic). The watermark can literally encode an electronic address of the related content object, but more typically encodes an index value that identifies a database record containing that address information. Application 09/571,422 details a number of connected-content applications and techniques.

One problem that arises in many watermarking applications is that of object corruption. If the object is reproduced, or distorted, in some manner such that the content presented for watermark decoding is not identical to the object as originally watermarked, then the decoding process may be unable to recognize and decode the watermark. To deal with such problems, the watermark can convey a reference signal. The reference signal is of such a character as to permit its detection even in the presence of relatively severe distortion. Once found, the attributes of the distorted reference signal can be used to quantify the content's distortion. Watermark decoding can then proceed – informed by information about the particular distortion present.

The assignee's applications 09/503,881and 09/452,023 detail certain reference signals, and processing methods, that permit such watermark decoding even in the presence of distortion. In some image watermarking embodiments, the reference signal comprises a constellation of quasi-impulse functions in the Fourier magnitude domain, each with pseudorandom phase. To detect and quantify the distortion, the watermark decoder converts the watermarked image to the Fourier magnitude domain and then performs a log polar resampling of the Fourier magnitude image. A generalized matched filter correlates the known orientation signal with the re-sampled watermarked signal to

find the rotation and scale parameters providing the highest correlation. The watermark decoder performs additional correlation operations between the phase information of the known orientation signal and the watermarked signal to determine translation parameters, which identify the origin of the watermark message signal. Having determined the rotation, scale and translation of the watermark signal, the reader then adjusts the image data to compensate for this distortion, and extracts the watermark message signal as described above.

With the foregoing by way of background, the specification next turns to the various improvements. It will be recognized that these improvements can typically be employed in many applications, and in various combinations with the subject matter of the patent documents cited herein.

DETAILED DESCRIPTION

Watermarks and Article Authentication

Some applications can employ watermark technology both for connected content/linking purposes, and for security/authenticity checking as well. Consider collectable sports paraphernalia as one example. (The same principles are naturally applicable on a much broader basis.)

It has been proposed that such paraphernalia be watermarked to assign each item a unique number (e.g., of a limited edition). Such marking can be effected by texturing (e.g., by engraving, etc.), printing (e.g., by silk-screen or otherwise, etc.). To assure that such marking isn't copied onto counterfeit articles, it desirably uses a watermark that does not survive copying (so-called "frail" watermarking). Examples of such frail watermarking are shown in copending applications 09/498,223, 09/645,779, 60/232,163, 09/689,289, 09/689,293, 09/689,226, and 60/247,389. (Use of frail watermarks on trading cards is disclosed in application 09/630,243.)

The process may work as follows:

1. Company X embeds 500 baseballs with 500 unique watermarks/id's.

2.The baseballs are distributed to retail outlets and sold.

3. The baseballs are packaged with material explaining what the watermark is and how it works.

4. The buyer opens the package and holds the baseball up to a web cam.

5. The default site for this is the "Register Your Mike McGwire Baseball" (or whatever) page.

6. After the buyer registers the baseball they are sent to a new page that is the provenance page for the baseball.

7. Since all watermarks/baseballs are unique, each time going forward the buyer holds up the ball he/she goes to the page that says "Yep this one is real."

8. Company X changes the destination page to which that baseball thereafter links (e.g., by changing the entry in a redirection database).

UV Watermarks

Certain printing contexts pose special challenges for digital watermarking. A case in point is certain product packaging, which may use a spot color fill over the entire package and may be inked by only one plate in the printing process. In this case, the variations in the printing needed to convey the watermark might be effected only by small areas that are devoid of ink. This is unsatisfactory in various applications.

To redress this, the watermarking can be effected using UV ink. Some of the UV spectrum is detected by the CCD or CMOS detector of most cameras under normal lighting. The effect can be enhanced by illuminating the object with black light in order to fluoresce the mark at the time of imaging – making the mark visible to the user and the camera.

Such an arrangement is well suited for in-store kiosks where a black light can be positioned with the camera. The kiosk may be arranged to that the user never sees the black light-illuminated UV watermark since it will be facing away from them as they present the watermark to the camera.

There are two different types of UV inks.

The first, and more generally applicable, type of UV ink is a conventional printing ink – used like other inks. Such inks typically fluoresce blue, orange, yellow and green. Various usages are possible. One is to print just the UV ink, with no normal ink below it, so the media appears unprinted. Another is to overprint other ink (e.g., conventional package markings) with the UV ink. Yet another is to print the UV ink over an un-

watermarked flood of black or other ink. Still another is to print one watermark using conventional ink, and overprint on it a second watermark pattern using UV ink. The second watermark pattern can be the same as the first pattern, or different (e.g., conveying the same watermark payload, or a different one).

The second type of UV ink is a lacquer that is commonly used for protecting images - typically outdoors like billboards, corrugated containers and other signage - from sun damage. This coating is put on after the object is printed, e.g., as a totally separate process, and then cures for some amount of time. Such lacquers are fairly viscous, forming relatively thick coatings. The thickness of the coating can be locally varied to change the surface topology of the object and thereby encode a watermark. For example, the lacquer can be uniformly applied in a first coat. Then a second, patterned, coat can be applied, depositing lacquer in some regions, and depositing none in others. With even a difference of a few microns, sufficient optical (and UV) distinctions can be detected between the regions to permit decoding of a watermark. (While the arrangement just described yields a binary watermark – with pels either "on" or "off" - similar techniques can be employed to effect a gray-scale-like encoding, e.g., by depositing lacquer in a range of intermediate thicknesses in different regions, or through use of a digital press.

Earlier disclosure relating to use of UV inks is provided in copending application 09/562,516. Patent 5,850,481 includes claims directed to texturing the microtopology of a surface to convey a watermark.

Watermarking by Article Shaping

The example just-given focused on UV inks and coatings as means to convey watermarks. The latter-discussed concept of applying different layers of material to encode a watermark, however, is applicable with materials other than UV inks. Any material that can be selectively deposited or printed to yield a controllable surface texture can similarly be applied. The scale of the surface texture, and component pel size, is application dependent. (Pel here refers to a pixel-like component that may be utilized in certain watermarks, e.g., in forming rectangular patterns that can be tiled over a surface.

Such arrangements are further detailed, e.g., in patent 5,862,260 and other references cited above.)

Moreover, the local variations can be effected by selectively removing or indenting a material, rather than simply adding a supplemental material.

To apply materials, various known ink printing technologies can be employed. On a smaller scale, techniques such as chemical vapor deposition can be utilized. To selectively remove or indent materials, techniques such as etching (chemical or plasma) and engraving can be used. Photolithography on photosensitive media, with subsequent development and removal of exposed (or unexposed) areas are other options.

The use of high-pressure intaglio techniques to texture paper is disclosed in laid-open application WO 200045344 and in pending application 09/127,502.

Blank Substrate Watermarking

In various of the assignee's prior applications, the notion of tinting blank paper substrate with a watermark was disclosed (e.g., applications 09/127,502 and 09/631,409). Many printers, however, cannot print to the margin of paper due to interference by pinch-rollers, or other paper-handling mechanisms. If a paper is tinted with a watermark, but the watermark does not extend to the edge of the page, the invisibility of the watermark is compromised by the contrast with the bordering, un-marked part of the page.

One approach is simply to exploit this visual feature – publicizing that it signifies that the page is watermarked.

A curative approach is to taper-off the watermark intensity towards the edges of the page, so a smooth transition between marked and unmarked regions may be effected. This will compromise readability near the edge of the page, but that is an acceptable trade-off in most applications.

Another approach is to pre-mark the blank paper at the margins, e.g., by the paper producer. The margin can be printed with a watermark that conveys just the reference (orientation/grid) signal.

Yet another approach is to pre-mark the entire page, e.g., by the paper manufacturer or distributor (e.g., Xerox or HP). All pages in a package (e.g., of 100 sheets) may be marked identically. An informational page can be automatically

generated for that package by a variable data printer. In addition to including the unique code associated with that pack, the informational page also tells the consumer how to register the URL for those unique watermarks, e.g., by visiting www.mymarc.com. This page is inserted into each pack, and the package is distributed through the normal retail channels. (In-store kiosks may be used to facilitate user registration of purchased paper packs.) When the user purchases the pack, he or she visits the mymarc.com site and specifies the URL to which that uniquely-marked paper should link.

Of course, it is not just letterhead or the like that can be premarked. Any printing stock can be processed to pre-encode a watermark, including greeting card stock, business card stock, direct mail inserts, etc.

Watermarks and Wristwatches, etc.

In applications 09/670,114 and 09/151,492, the present assignee detailed how watermarks can be employed on everyday objects, such as wristwatches, and serve to enable additional features.

The detailed embodiments noted that a watermark pattern can be engraved into an exterior surface of such an item. But other arrangements are possible. Consider digital watches, or other devices with electronic displays. A watermark pattern can be formed by the display itself, by controlling individual pixels accordingly. Different patterns can be made to appear on the screen in order to provide different functionality.

Taking the case of a digital wristwatch, it is familiar that many different features and modes can be set by manipulation of a few simply user interface controls – such as buttons. In accordance with this aspect of the invention, one mode can set the watch to display a first watermark pattern. The user can present the wristwatch display to a webcam, which senses the displayed pattern, decodes the watermark therefrom, and triggers a corresponding action. The action corresponding to the first watermark pattern can be to link an associated internet device to a personalized web site relating to the user's fitness training (e.g., as further detailed in the '114 application).

Similarly, by further manipulation of the device's user interface, a second watermark pattern can be made to appear on the watch display. When this pattern is

sensed by a webcam, a different response can be triggered (e.g., access to a web-based email account associated with the user).

While the responses just-detailed are tailored to the particular user, other patterns can trigger responses that are the same for a class of users, or for all users. Examples include linking to CNN headlines, weather information, etc., etc.

To trigger custom responses, custom watermark payloads – unique to that user – can be employed. This can be achieved by device serialization, e.g., assigning each wristwatch a different ID number, and deriving unique watermark payloads from such ID. (Suitable measures must be taken to assure that user privacy is respected.)

Another way of triggering user-customized responses does not rely on serialization of the wristwatch. Instead, the responding- or linking-system (e.g., a PC, camera-equipped cell phone, etc.) can include data specific to the user. Thus, all wristwatches may display the same watermark pattern when put in the "link-to-personal-training-website" mode. John's computer can respond to this payload by linking to www.address.com/john_fitness, whereas Jane's computer can respond to this same payload by linking to www.address.com/jane_fitness.html - based on customization data resident in the associated device.

In still other arrangements, the wristwatch (or PDA) screen can show an image such as a picture of the PDA's owner. The picture can be watermarked to serve as a business card. This picture can be beamed to an associate's device (e.g., PDA) at conferences, for example. When the associate gets back to an online computer he can hold up the picture (or digitally submit to a watermark reader) and link directly to the first person's contact page or similar destination for sales, etc.

This can also be used as a viral promotions opportunity where people start beaming the watermarked image to anybody else that has a PDA. Picture a crowd of friends or colleagues at MacWorld. The new recipients hold their PDA up to a webcam at a kiosk or at the office. A pollination or diaspora effect ensues. Take this one step further and, when a user beams the watermarked picture to another device, he also beams a small application with it that modifies the watermark each time it's beamed. The modification could change the payload so that there may be, e.g., 10,000 different payloads. Each time it's beamed, the watermark changes within the parameters of this

10,000 unit payload. One of these payloads is a winner once you check it online in the promotion. The idea is to generate traffic across many PDAs and get them all to check if their mark is the winner.

One advantage to such arrangements is that the wristwatch housing does not need to be custom fabricated. Another is that the watermark can be controlled to present a number of different payloads, rather than a single, unchanging, payload.

Watermarks and Transaction Cards

In application 09/562,049, the assignee disclosed how a consumer's physical custody of a credit card can be verified - when making on-line purchases - by showing the credit card to a camera-equipped system that reads a verification watermark from the card face.

To deter use of precision photocopy apparatuses to reproduce credit card faces (with associated watermark), the face of the card can be provided a reflective layer, e.g., in the form of an overlay or varnish. In the bright illumination of a photocopier, such layer mirrors the light back onto the photodetectors, preventing them from accurately reproducing the watermark pattern. In contrast, when presented to a web cam or other such imaging device, no bright illumination is typically present, so the photosensors are not overwhelmed and the card can be used for its intended authentication purpose.

If a home PC web cam, or other imaging device, is used to capture an image of the card – to confirm its physical presentment – the same imaging device can be used to acquire an image of the user (only with user permission...) This image can be transmitted to the on-line merchant and stored in association with the transaction record. Automated pattern recognition techniques can be used to confirm that the image captured and logged in the merchant's computer is, in fact, a face. If it later turns out that the card was stolen, on-line merchants with which it was used may have an image of the perpetrator.

It may be desirable to incent authenticated on-line credit card transactions by providing a reward to consumers who participate in the desired manner. Thus, for example, a consumer that demonstrates physical custody of a credit card by presenting same to a camera (and having the watermark decoded, etc.), may receive a 0.5%

discount. If the consumer further consents to capture and storage of a facial image, the consumer may receive a 1% discount, etc.

Alternatively, the incentive may be offered to the merchant, by the charge card company.

In a variant arrangement, the watermark reader can read the watermark and also capture image data unique to the card / camera combination. The data is submitted to an authentication server and thus becomes a "signature" for that transaction. Any form of attack that attempts to replay the transaction at a later time will fail because of duplicate signature. Because the actual card image is not used, it cannot be captured as a form of attack. Furthermore, a scanned image of a card used to circumvent the system would have an unvaried signature and would thus trigger detection of the attack if used multiple times.

Watermarks and Software Licensing

A premise of the '049 application – remotely confirming possession of an object by use of watermark information decoded from the object – finds application beyond internet credit card usage.

One such other application is in software licensing. If a corporate enterprise buys a license entitling it to install a software program on 100 computers, it typically receives a single copy of the disk, and then installs the software on (hopefully) 100 computers or less.

The disk can be distributed with a watermarked card, or other talisman. (Or the disk itself can be watermarked.) Each time the software is installed on a computer, the card (or talisman, or disk) must be shown to an associated web cam. The computer decodes the watermark, transmits it to the software vendor, which then increments a tally detailing the number of installations made so far. If the number doesn't exceed the licensed number, the software vendor transmits-back a key or other data that permits the program to be utilized.

If the card is not shown to the camera, or if the card is shown 101 times, the software is inoperative.

Watermarks and Magnetic Recording Media

Magnetic recording media are well suited to steganography, such as digital watermarking.

While prior art teaches that minute variations (e.g., noise) inherent in a magnetic medium (e.g., a credit card stripe) can be used to uniquely identify the medium, it does not appear such slight variations have been effected deliberately to convey auxiliary, (convert) data.

The same functionality gained by watermarking of digital and physical objects (e.g., object identification, authentication, linking, etc.) can likewise be achieved by watermarking of magnetic media.

Watermarks Miscellania

The applications of watermarking extend far beyond those noted above. One is steganographic marking of circuit boards, e.g., to encode manufacturing information (fab date, mask identifiers, process parameters, alignment data) and security or authentication information. Alignment grid data, for example, can be printed on the board to facilitate navigation relative to the board, e.g., by automated parts placement devices and soldering apparatus. The grid can permit local estimates of board rotation and standoff distance from the optical sensor. Among the advantages from such approach are lower cost solder paste inspection systems; measurement reference plane can be determined from grid rather than performing height reconstructions over the entire board; faster and more accurate navigation of sensor or pick-and-place nozzle over board, and eliminating need for fiducial marks which waste previous board space.

Another application is watermarking of electronic components, such as integrated circuits, capacitors, resistors, etc. This would allow machine recognition of such parts, facilitating use in automated board stuffing equipment. The watermark may also convey information required for test or inspection, such as which algorithms to run, and what the applicable tolerances are.

In the foregoing arrangements, a camera may be integrated with the robotic arm or nozzle that places components on the board, or solders same. This offers improvements in speed and accuracy when compared with fixed camera systems.

Another is marking of public signage, e.g., street signs, with steganographic marking that can be sensed by automotive sensors and used, e.g., for navigation purposes.

While watermarking of physical objects is known from the assignee's prior applications, the objects can be those associated with rendering of electronic content. Thus, for example, computer screens (CRT and LCD) and projection system optical components can be formed to encode a static watermark on all content rendered on such device.

Counterfeiting of designer garments is big business. Such piracy can be deterred by watermarks. For example, a garment's hang-tag or ribbon-tag can be watermarked (e.g., by tinting, text steganography, etc.), and cross-checked against data memorialized elsewhere on the garment (e.g., a barcode on another tag, or a watermark formed by subtle changes to coloration or imagery on the garment). If these two data do not correspond in an expected manner, the garment may be presumed to be a knock-off.

In some applications, a watermark can be initially concealed, and revealed after usage. The soles of shoes, the tread of tires, any other media that wears-away can cover a watermark pattern, and reveal same only after a period of usage.

Watermarks and Action Triggering

Application 09/709,255 discloses use of watermark technology in connection with toys and dolls that provide "read-aloud" book functionality.

More generally, any mechanical device with a processor and some form of stored memory capable of holding a software program (that can make the machine behave in different manners) can respond to watermarks. The machine discussed can vary greatly in form factor, but – in addition to toys and dolls – can include industrial robots, home appliances, consumer electronic devices (e.g., VCR), etc.

In many cases, the ability of a human owner to actually access and trigger programming within the machine is limited by the form factor, the complexity of the interface or the capabilities of the owner / operator. In the first instance, consider a toy robot or doll with no traditional human input interface such as button controls, keyboard or mice. In the second instance, consider a device such as a VCR which has programming controls, but where the actual steps for programming are time consuming

or cumbersome for the owner (thus the permanently flashing 12:00:00 on the front display). In the third instance, the owner of a device such as a toy may not be able to execute complex instructions or even read the instructions due to age limitations, etc.

In accordance with this aspect of the invention, such a machine is provided with a booklet of instructions, each page of which is watermarked to serve as a programming "trigger." One page, for example, may have the trigger for setting a robot to dance. By flipping to the page, then holding the page up in front of the robot, the trigger is delivered via an onboard camera and reader. The robot then uses the watermark / trigger to retrieve the instruction set associated with the watermark and alters behavior accordingly. In the case of children's toys, the instructions could be in the form of pictographs. In this case, the child only needs to be instructed in how to select the desired action, then hold the booklet up to trigger the behavior.

Watermarks And Decryption

This aspect of the invention relates to protecting encrypted media, such as DVDs. There is a concern that if digital watermarking is used as a DVD copy control, it may be circumvented by building a DVD player that will decrypt the DVD, but will not detect the copy control digital watermarks -- rendering the copy control digital watermarks useless.

In accordance with this aspect of the invention, digital watermarking is tied to the decryption process. In a first implementation, a digital watermark associated with video frame n includes a plural-bit payload. The plural-bit payload includes a decryption key to decrypt a successive video frame n+1 (or n+2, etc.), or to decrypt an upcoming set of video frames. In order to obtain appropriate decryption keys for upcoming frames, a DVD player *must* decode the digital watermarks. Of course, the digital watermarks can be embedded in audio as well as video channels.

In a second implementation, a non-digital watermark detecting DVD player can still decode the video, but only a low fidelity version. A high fidelity version (e.g., surround sound, full color images, etc.) is only accessible from a key carried by a digital watermark payload. The high fidelity version is unlocked (or decrypted) with the digital watermark key.

To provide a comprehensive disclosure without unduly lengthening this specification, the patents and applications cited above are incorporated herein by references.

Having described and illustrated the subject technologies with reference to illustrative embodiments, it should be recognized that the invention is not so limited.

For example, while the detailed description focused on digital watermarks to convey auxiliary information with audio and video content, other techniques can be used as well (e.g., VBI, digital fingerprints, header meta data, etc.). Likewise, in embodiments relating to marking of physical objects, other machine-readable data representations can be employed (e.g., bar codes, glyphs, RF IDs, mag stripes, smart card technology, etc.).

The implementation of the functionality described above (including watermark decoding) is straightforward to artisans in the field, and thus not further belabored here. Conventionally, such technology is implemented by suitable software, stored in long term memory (e.g., disk, ROM, etc.), and transferred to temporary memory (e.g., RAM) for execution on an associated CPU. In other implementations, the functionality can be achieved by dedicated hardware, or by a combination of hardware and software. Reprogrammable logic, including FPGAs, can advantageously be employed in certain implementations.

It should be recognized that the particular combinations of elements and features in the above-detailed embodiments are exemplary only; the interchanging and substitution of these teachings with other teachings in this and the incorporated-by-reference patents/applications are also contemplated.

In view of the wide variety of embodiments to which the principles and features discussed above can be applied, it should be apparent that the detailed embodiments are illustrative only and should not be taken as limiting the scope of the invention. Rather, I claim as my invention all such modifications as may come within the scope and spirit of the following claims and equivalents thereof.